Claims

What is claimed is:

[c1] A method to support access control checks in a directory server with a chaining backend, comprising:

binding a user to a multiplexer;

forwarding an authentication sequence from the multiplexer to a first remote server;

binding the user to the first remote server;

authenticating the user if binding to the first remote server is successful;

binding the multiplexer as a special user to a second remote server, wherein the second remote server holds target data;

sending an operation and an original user identity from the user to the multiplexer; and

forwarding the operation from the multiplexer to the second remote server.

[c2] The method of claim 1, further comprising:

retrieving an access control information statement from an access control list stored on the second remote server; and

evaluating the operation by the second remote server using the access control statement of the user.

[c3] The method of claim 2, wherein the access control information statement is stored as an attribute of an entry on the second remote server.

[c4] The method of claim 3, wherein the access control information statement comprises a target and an access control rule.

[c5] The method of claim 1, further comprising:

retrieving an access control information statement from an access control list stored on the multiplexer; and

evaluating the operation by the multiplexer using the access control statement of the user.

[c6] The method of claim 5, wherein the access control information statement is stored as an attribute of an entry on the multiplexer.

[c7] The method of claim 6, wherein the access control information statement comprises a target and an access control rule.

[c8] The method of claim 1, wherein forwarding the authentication sequence to the first remote server occurs when a realm value sent in a digest challenge is not interpreted by the directory server, a target host name field of a digest response is not checked by the directory server, and the first remote server is part of a common realm.

[c9] The method of claim 1, wherein the operation comprises an internal operation portion and an external operation portion.

[c10] The method of claim 9, further comprising:

chaining the internal operation portion based on an identity of a component issuing the internal operation.

[c11] The method of claim 2, further comprising:

enabling retrieval of the access control information statement on a remote server basis.

[c12] The method of claim 2, further comprising:
disabling retrieval of the access control information statement on a remote server basis.

[c13] The method of claim 6, further comprising:
retrieving the entry to evaluate an access control list on the multiplexer.

[c14] The method of claim 13, wherein the entry comprises a user.

[c15] The method of claim 13, wherein the entry comprises a group.

[c16] A computer system to support access control checks in a directory server with a chaining backend, comprising:
a processor;
a memory; and
software instructions stored in the memory for enabling the computer system under control of the processor, to perform:
binding a user to a multiplexer;
forwarding an authentication sequence from the multiplexer to a first remote server;
binding the user to the first remote server;
authenticating the user if binding to the first remote server is successful;
binding the multiplexer as a special user to a second remote server, wherein the second remote server holds target data;
sending an operation and an original user identity from the user to the multiplexer; and
forwarding the operation from the multiplexer to the second remote server.

[c17] The computer system of claim 16, wherein the software instructions further comprise instructions to perform:

retrieving an access control information statement from an access control list stored on the second remote server; and

evaluating the operation by the second remote server using the access control statement of the user.

[c18] The computer system of claim 16, wherein the software instructions further comprise instructions to perform:

retrieving an access control information statement from an access control list stored on the multiplexer; and

evaluating the operation by the multiplexer using the access control statement of the user.

[c19] An apparatus to support access control checks in a directory server with a chaining backend, comprising:

means for binding a user to a multiplexer;

means for forwarding an authentication sequence from the multiplexer to a first remote server;

means for binding the user to the first remote server;

means for authenticating the user if binding to the first remote server is successful;

means for binding the multiplexer as a special user to a second remote server, wherein the second remote server holds target data;

means for sending an operation and an original user identity from the user to the multiplexer; and

means for forwarding the operation from the multiplexer to the second remote server.

[c20] The apparatus of claim 19, further comprising:

means for retrieving an access control information statement from an access control list stored on the second remote server; and

means for evaluating the operation by the second remote server using the access control statement of the user.

[c21] The apparatus of claim 19, further comprising:

means for retrieving an access control information statement from an access control list stored on the multiplexer; and

means for evaluating the operation by the multiplexer using the access control statement of the user.